Novel Constructions of Complex Orthogonal Designs for Space-time Block Codes

Yuan Li, Chen Yuan, and Haibin Kan*
Shanghai Key Lab of Intelligent Information Processing,
School of Computer Science, Fudan University,
Shanghai 200433, P. R. China.
*hbkan@fudan.edu.cn

***Abstract*—Complex orthogonal designs (CODs) are used to construct space-time block codes in wireless transmission. COD $\mathcal{O}_z$ with parameter $[p, n, k]$ is a $p \times n$ matrix, where nonzero entries are filled by $\pm z_i$ or $\pm z_i^*$, $i = 1, 2, \ldots, k$, such that $\mathcal{O}_z^H \mathcal{O}_z = (|z_1|^2 + |z_2|^2 + \ldots + |z_k|^2) I_{n\times n}$. In practice, n is the number of antennas, k/p the code rate, and p the decoding delay.**

One fundamental problem is to construct COD to maximize k/p and minimize p when n is given. Recently, this problem is completely solved by Liang and Adams et al. It's proved that when $n = 2m$ or $2m - 1$, the maximal possible rate is $(m+1)/(2m)$ and the minimum delay $\binom{2m}{m-1}$(with the only exception $n \equiv 2 \pmod 4$ where it is $2\binom{2m}{m-1}$). However, when the number of antennas increase, the minimum delay grows fast and eats the otherwise fast decoding. For example, when $n = 14$ the minimal delay for a code with maximal rate is 6006!

Therefore, it is very important to study whether it is possible, by lowering the rate slightly, to shorten the decoding delay considerably. In this paper, we demonstrate this possibility by constructing a series of CODs with parameter

$$[p, n, k] = \left[\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}\right],$$

where $0 \le w \le n$.

Besides that, all optimal CODs, which achieve the maximal rate and minimal delay, are contained in our explicit-form constructions. And this is the first explicit-form construction, while the previous are recursive or algorithmic.

I. INTRODUCTION

Space-time block codes have been widely investigated for wireless communication systems with multiple transmit and receive antennas. Since the pioneering work by Alamouti [7] in 1998, and the work by Tarokh et al. [22], [23], orthogonal designs have become an effective technique for the design of space-time block codes (STBC). The importance of this class of codes comes from the fact that they achieve full diversity and have the fast maximum-likelihood (ML) decoding.

A complex orthogonal design (COD) $\mathcal{O}_z[p, n, k]$ is an $p \times n$ matrix, and each entry is filled by $\pm z_i$ or $\pm z_i^*$, $i = 1, 2, \ldots, k$, such that $\mathcal{O}_z^H \mathcal{O}_z = \sum_{i=1}^n |z_i|^2 I_n$, where H is the Hermitian transpose and I_n is the $n \times n$ identity matrix. Under this definition, the designs are said to be combinatorial, in the sense that there is no linear processing in each entry. When linear combination of variables are allowed, we call it generalized complex orthogonal design (GCOD).

Code rate k/p and decoding delay p are the two most important criteria of complex orthogonal space-time block codes. One important problem is, given n, determine the tight upper bound of code rate, which is called maximal rate problem. Another is, given n, determine the tight lower bound of decoding delay p when code rate k/p reaches the maximal, which is called minimal delay problem.

For combinatorial CODs, where linear combination is not allowed, Liang determined for a COD with $n = 2m$ or $2m - 1$, the maximal possible rate is $\frac{m+1}{2m}$ [14]. Liang gave an algorithm in [14] to generate such CODs with rate $\frac{m+1}{2m}$, which shows that this bound is tight. In [15], Yuan et al. simplifies Liang's proof on the upper bound of code rate slightly. The minimal delay problem are solved by Adams et al. In [5], lower bound $\binom{2m}{m-1}$ of decoding delay is proved for any $n = 2m$ or $2m - 1$. In [6], Adams et al. prove that when $n \equiv 2 \pmod 4$, decoding delay p is lowered bound by $2\binom{2m}{m-1}$.

Besides some scattered constructions for relatively small number of antennas n [25], [22], [19], several general methods to construct CODs have been proposed. Liang's algorithmic construction in [14] achieves the maximal rate for all n, acheives the minimal delay when $n \equiv 1, 2, 3 \pmod 4$. But when $n \equiv 0 \pmod 4$, the delay is twice of the minimal delay. In [20], a different algorithmic method to generate complex orthogonal is proposed, which has the same code rate and decoding delay as Liang's construction. In [16], a closed-form iterative construction of complex orthogonal designs was proposed, which achieves both the maximal rate and minimal delay.

The unfortunate property of COD is that for $n = 2m$ or $2m - 1$ transmit antennas, the codes with maximal rate $(m + 1)/(2m)$ has minimal decoding delay $\binom{2m}{m-1}$ (with exception $n = 2 \pmod 4$ where it is $2\binom{2m}{m-1}$). For example, when $n = 14$, the minimal delay for a code with maximal rate is 6006! Therefore, it's meaningful to construct CODs with smaller decoding delay by sacrificing code rate and investigate the tradeoff between code rate and decoding delay.

In this paper, we demonstrate it's possible to shorten the decoding delay considerably by lowering the rate slightly. This is achieved by constructing new CODs with parameter $[p, n, k] = \left[\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}\right]$, where $0 \le w \le n$. Besides that, all optimal CODs, which achieve the maximal rate and minimal delay, are contained in our explicit-form

978-1-4673-0775-8/12/$31.00 ©2012 IEEE

constructions. And this is the first explicit-form construction, while the previous are either recursive or algorithmic.

The organization of our paper is as follows. In section 2, we introduce the notions and definitions which will be used. In section 3, we present our explicit-form constructions. In section 4, an upper bound of $A_{\mathbb{C}}(R,n)$, which is the minimum number p for which there exists a COD of size $p\times n$ and rate at least R, is obtained as a consequence of our explicit-form construction. In section 5, we give the conclusion.

II. Preliminaries

In this section, we introduce some basic notions, which will be used in the sequel.

$\mathbb{C}$ denotes the field of complex numbers, $\mathbb{R}$ the field of real numbers and $\mathbb{F}_2$ the field with two elements. Adding over $\mathbb{F}_2$ is denoted by $\oplus$ to avoid ambiguity. All vectors are assumed to be column vectors. For any field $\mathbb{F}$, denoted by $\mathbb{F}^n$ and $M_{m\times n}(\mathbb{F})$ the set of all n-dimensional vectors in $\mathbb{F}$ and the set of all $m\times n$ matrices in $\mathbb{F}$, respectively. For any vector $x\in\mathbb{F}^n$, denote by x^T the transpose of x. For any matrix $A\in M_{m\times n}(\mathbb{C})$, denote by A^T the transpose of A and by A^H the conjugate transpose of A. Denote by

$$A(i_1,i_2,\ldots,i_p;j_1,j_2,\ldots,j_q)$$

and

$$A(s_1,\ldots,s_2;t_1,\ldots,t_2)$$

the submatrix consisting of i_1^{th}, i_2^{th}, …, i_p^{th} rows and the j_1^{th}, j_2^{th}, …, j_q^{th} columns of A, and the submatrix consisting of the s_1^{th}, $(s_1+1)^{\text{th}}$, …, s_2^{th} rows and the t_1^{th}, $(t_1+1)^{\text{th}}$, …, t_2^{th} columns of A, where $s_1<s_2$ and $t_1<t_2$, respectively. We use $A(i,j)$ for the (i,j) element of the matrix A. In this paper, rows and variables are often indexed by vectors in $\mathbb{F}_n^2$.

For convenience, let $e_i\in\mathbb{F}_2^n$ be the vector with i^{th} bit occupied by 1 and the others 0, i.e., $e_i=(\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i})$ and let $e=e_1\oplus e_2\oplus\ldots\oplus e_n$, i.e., $e=(1,1,\ldots,1)_2$.

The weight of a vector in $\mathbb{F}_2^n$ is defined as the number of ones in n bits, i.e., $\text{wt}(\alpha)=\sum_{i=1}^n\alpha(i)$. Furthermore, $\text{wt}_{s,t}(\alpha)$ is defined as the sum of s^{th} bit to t^{th} bit, i.e.,

$$\text{wt}_{s,t}(\alpha)=\sum_{i=s}^{t}\alpha(i).$$

Definition 1. *A $[p,n,k]$ complex orthogonal design $\mathcal{O}_z$ is a $p\times n$ rectangular matrix whose nonzero entries are*

$$z_1,z_2,\ldots,z_k,-z_1,-z_2,\ldots,-z_k$$

or their conjugates

$$z_1^*,z_2^*,\ldots,z_k^*,-z_1^*,-z_2^*,\ldots,-z_k^*,$$

where $z_1,z_2,\ldots,z_k$ are indeterminates over $\mathbb{C}$, such that

$$\mathcal{O}_z^H\mathcal{O}_z=(|z_1|^2+|z_2|^2+\cdots+|z_k|^2)I_{n\times n}.$$

k/p is called the code rate of $\mathcal{O}_z$, and p is called the decoding delay of $\mathcal{O}_z$.

A matrix is called an Alamouti 2×2 if it matches the following form

$$\begin{pmatrix} z_i & z_j \\ -z_j^* & z_i^* \end{pmatrix}, \tag{1}$$

up to negation or conjugation of z_i or z_j. We say two rows share an Alamout 2×2 if and only if the intersection of the two rows and some two columns form an Alamouti 2×2.

Definition 2. *The equivalence operations performed on any COD are defined as follows.*

1) Rearrange the order the rows("row permutation").
2) Rearrange the order the columns ("column permutation").
3) Conjugate all instances of certain variable ("instance conjugation").
4) Negate all instances of certain variable ("instance negation").
5) Change the index of all instances of certain variable ("instance renaming").
6) Multiply any row by -1, ("row negation").
7) Multiply any column by -1, ("column negation").

It's not difficult to verify that, given a COD $\mathcal{O}_z[p,n,k]$, after arbitrary equivalence operations, we will obtain another COD $\mathcal{O}'_z[p,n,k]$. And we say COD $\mathcal{O}_z$ and $\mathcal{O}'_z$ are the same under equivalence operations.

Following the definition in [14], define an $(n_1,n_2)-\mathcal{B}_j$ form by

$$\mathcal{B}_j = \begin{pmatrix} z_jI_{n_1} & \mathcal{M}_1 \\ -\mathcal{M}_1^H & z_j^*I_{n_2}\end{pmatrix} = \left(\begin{array}{cccc|cccc} z_j & 0 & \cdots & 0 & & & & \\ 0 & z_j & \cdots & 0 & & & & \\ \vdots & \vdots & \ddots & \vdots & & \mathcal{M}_j & & \\ 0 & 0 & \cdots & z_j & & & & \\ \hline & & & & z_j^* & 0 & \cdots & 0 \\ & & & & 0 & z_j^* & \cdots & 0 \\ & -\mathcal{M}_j^H & & & \vdots & \vdots & \ddots & \vdots \\ & & & & 0 & 0 & \cdots & z_j^* \end{array}\right) \tag{2}$$

where $n_1+n_2=n$. And we call it $\mathcal{B}_j$ form for short.

Definition 3. *[5] We say COD $\mathcal{O}_z$ is in $\mathcal{B}_j$ form if the submatrix $\mathcal{B}_j$ can be created from $\mathcal{O}_z$ through equivalence operations except for column permutation. Equivalently, $\mathcal{O}_z$ is in $\mathcal{B}_j$ form if every row of $\mathcal{B}_j$ appears within the rows of $\mathcal{O}_z$, up to possible conjugations of all instances of z_i and possible factors of -1.*

It is proved that [5] that COD $\mathcal{O}_z$ is in some $\mathcal{B}_j$ form if and only if one row in $\mathcal{O}_z$ matches one row of $\mathcal{B}_j$ up to signs and conjugations.

In [14], Liang proved the upper bound $\frac{m+1}{2m}$ of code rate $\frac{k}{p}$ for any $n=2m$ or $2m-1$, and obtained the necessary and sufficient condition to reach the maximal rate.

Theorem 4. *Let $n=2m$ or $2m-1$. The rate of COD $\mathcal{O}_z[p,n,k]$ is upper bounded by $\frac{m+1}{2m}$, i.e., $\frac{k}{p}\le\frac{m+1}{2m}$.*

This bound is achieved if and only if for all $i = 1, 2, \ldots, k$, $\mathcal{B}_j$ is an $(m, m-1)$-$\mathcal{B}_j$ or $(m-1, m)$-$\mathcal{B}_j$ form and there are no zero entries in $\mathcal{M}_j$, when $n = 2m-1$; $\mathcal{B}_j$ is an (m, m)-$\mathcal{B}_j$ form and there are no zero entries in $\mathcal{M}_j$, when $n = 2m$.

The lower bound on the decoding delay when code rate reaches the maximal is completely solved by Adams et al. in [5] and [6].

Theorem 5. *Let $n = 2m$ or $2m-1$. For COD $\mathcal{O}_z[p, n, k]$, if the rate reaches the maximal, i.e., $\frac{k}{p} = \frac{m+1}{2m}$, the delay, i.e., p, is lower bounded by $\binom{2m}{m-1}$ when $n \equiv 0, 1, 3 \pmod 4$; by $2\binom{2m}{m-1}$ when $n \equiv 2 \pmod 4$.*

The technique in proving the lower bound $\binom{2m}{m-1}$ is the observation and definition of zero pattern, which is a vector in $\mathbb{F}_2^n$ defined with respect to one row where the i^{th} bit is 0 if and only if the element on column i is 0. For example, when

$$\mathcal{O}_z = \begin{pmatrix} z_1 & z_2 & z_3 \\ -z_2^* & z_1^* & 0 \\ -z_3^* & 0 & z_1^* \\ 0 & z_3^* & -z_2^* \end{pmatrix}, \tag{3}$$

the first row has zero pattern $(1, 1, 1)$, the second $(1, 1, 0)$, the third $(1, 0, 1)$, the fourth $(0, 1, 1)$.

III. Explicit-form Constructions

In this section, we present explicit-form constructions of M-type CODs. The basic idea is first to construct a basic COD with rate $1/2$ and parameters $[2^{n+1}, n, 2^n]$, which are based on combinatorial methods by using vectors in $\mathbb{F}_2^{n+1}$. Then, by choosing submatrices from the basic COD, we obtain CODs with paramters

$$[p, n, k] = \left[\binom{n}{w-1} + \binom{n}{w+1}, n, \binom{n}{w}\right],$$

where $-1 \le w \le n+1$. Note that, when $n \not\equiv 0 \pmod 4$, all maximal-rate, minimal-delay CODs are contained in the above constructions.

Next, we consider $n \equiv 0 \pmod 4$. By padding an extra column on our basic COD, we obtain COD with parameter $[2^n, n, 2^{n-1}]$. Again, by choosing submatrices from the basic COD, we obtain CODs with parameters $[\binom{n}{n/2+1}, n, \binom{n-1}{n/2-1}]$, which contains the codes with maximal rate and minimal decoding delay.

Theorem 6. *Let $\mathcal{G}_n$ be $2^{n+1} \times n$ matrix, where rows are indexed by vectors in $\mathbb{F}_2^{n+1}$ and columns are indexed by $1, 2, \ldots, n$. For all $\alpha \in \mathbb{F}_2^{n+1}, 1 \le i \le n$,*

- *if $\alpha(i) = 0$, then $\mathcal{G}_n(\alpha, i) = 0$,*
- *if $\alpha(i) = 1$ and $\alpha(n+1) = 0$, then $\mathcal{G}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z_{\varphi(\alpha,i)}$,*
- *if $\alpha(i) = 1$ and $\alpha(n+1) = 1$, then $\mathcal{G}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z^*_{\varphi(\alpha,i)}$,*

where

$$\theta(\alpha, i) = \begin{cases} wt_{i,n+1}(\alpha) + \frac{i}{2}, & \text{if } i \text{ is even}, \\ wt_{i,n+1}(\alpha) + \frac{i-1}{2} + \alpha(n+1), & \text{if } i \text{ is odd}, \end{cases} \tag{4}$$

and

$$\begin{aligned} \varphi(\alpha, i) &= \alpha \oplus \alpha(n+1)e \oplus e_i \\ &= (\alpha(1) \oplus \alpha(n+1), \ldots, \alpha(i) \oplus \alpha(n+1) \oplus 1, \ldots, \\ &\quad \alpha(n+1) \oplus \alpha(n+1)). \end{aligned}$$

Then $\mathcal{G}_n$ is a COD with parameter $[2^{n+1}, n, 2^n]$.

Proof: It is sufficient to prove 1) every variable, up to negation or conjugation, appears exactly once in each column; 2) any two different columns are orthogonal.

Since for fixed i, $\varphi(\alpha, i)$ takes nonzero values on 2^n different vectors $\alpha \in \mathbb{F}_2^{n+1}, \alpha(i) = 1$. To prove 1), we only need to show φ is a surjective, i.e. $\alpha \ne \beta \Rightarrow \varphi(\alpha, i) \ne \varphi(\beta, i)$. Suppose to the contrary that there exists α and β where $\alpha \ne \beta$, $\alpha(i) = \beta(i) = 1$ and $\varphi(\alpha, i) = \varphi(\beta, i)$. Expanding $\varphi(\alpha, i) = \varphi(\beta, i)$ by definition, we have

$$\alpha \oplus \alpha(n+1)e \oplus e_i = \beta \oplus \beta(n+1)e \oplus e_i,$$

which is equivalent to

$$\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e.$$

If $\alpha(n+1) = \beta(n+1)$, then $\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e = 0 \Rightarrow \alpha = \beta$, which is contradicted with $\alpha \ne \beta$. If $\alpha(n+1) \ne \beta(n+1)$, then $\alpha \oplus \beta = (\alpha(n+1) \oplus \beta(n+1))e = e$, which is contradicted with $\alpha(i) = \beta(i) = 1$.

To prove any two different columns are orthogonal, it is sufficient to show that, every pair of nonzero entries in the same row are in an Alamouti 2×2.

Let columns $1 \le i < j \le n$ and $\alpha \in \mathbb{F}_2^{n+1}$ be any row, satisfying $\alpha(i) = \alpha(j) = 1$. Let $\gamma = \varphi(\alpha, i)$, $\delta = \varphi(\alpha, j)$. Since every variable appears exactly once in each column, we assume $z[\delta]$ appears in the β^{th} row in i^{th} column, i.e., $\varphi(\beta, i) = \gamma$.

By the assumption that $z[\delta]$ appears in $\mathcal{G}_n(\beta, i)$, we have $\varphi(\beta, i) = \varphi(\alpha, j)$, i.e.,

$$\alpha \oplus \alpha(n+1)e \oplus e_j = \beta \oplus \beta(n+1)e \oplus e_i,$$

which implies

$$\begin{aligned} \beta &= \alpha \oplus \alpha(n+1)e \oplus e_j \oplus \beta(n+1)e \oplus e(i) \\ &= \alpha \oplus (\alpha(n+1) \oplus \beta(n+1))e \oplus e_i \oplus e_j. \end{aligned} \tag{5}$$

Noting that φ takes nonzero value on (α, i), (α, j) and (β, i), we have $\alpha(i) = \alpha(j) = \beta(j) = 1$. Considering i^{th} value in equality (5), we conclude $\alpha(n+1) \oplus \beta(n+1) = 1$. Thus,

$$\alpha \oplus \beta = e \oplus e_i \oplus e_j. \tag{6}$$

Taking $\beta = \alpha \oplus e \oplus e_i \oplus e_j$ into $\varphi(\beta, j)$, we have

$$\begin{aligned}\varphi(\beta, j) &= \beta \oplus \beta(n+1)e \oplus e_j \\ &= \alpha \oplus \alpha(n+1)e \oplus e_j \oplus \beta(n+1)e \oplus e_i \oplus \\ &\quad\ \beta(n+1)e \oplus e_j \\ &= \alpha \oplus \alpha(n+1)e \oplus e_i \\ &= \varphi(\alpha, i).\end{aligned}$$

Therefore, submatrix $\mathcal{G}_n(\alpha, \beta; i, j)$ could be written in either of the two following forms

$$\begin{pmatrix}(-1)^{\theta(\alpha,i)}z_\gamma & (-1)^{\theta(\alpha,j)}z_\delta \\ (-1)^{\theta(\beta,i)}z_\delta^* & (-1)^{\theta(\beta,j)}z_\gamma^*\end{pmatrix}$$

or

$$\begin{pmatrix}(-1)^{\theta(\alpha,i)}z_\gamma^* & (-1)^{\theta(\alpha,j)}z_\delta^* \\ (-1)^{\theta(\beta,i)}z_\delta & (-1)^{\theta(\beta,j)}z_\gamma\end{pmatrix}.$$

Now we calculate $\theta(\alpha, i) + \theta(\alpha, j) + \theta(\beta, i) + \theta(\beta, j)$ to check whether it is an Alamouti 2×2.

First, we calculate $\theta(\alpha, i) + \theta(\beta, i)$ according to the parity of i. When i is even,

$$\begin{aligned}&\theta(\alpha, i) + \theta(\beta, i) \\ &= \mathrm{wt}_{i,n+1}(\alpha) + \frac{i}{2} + \mathrm{wt}_{i,n+1}(\beta) + \frac{i}{2} \\ &\equiv \mathrm{wt}_{i,n+1}(\alpha \oplus \beta) + i.\end{aligned}$$

When i is odd,

$$\begin{aligned}&\theta(\alpha, i) + \theta(\beta, i) \\ &= \mathrm{wt}_{i,n+1}(\alpha) + \frac{i-1}{2} + \alpha(n+1) + \\ &\quad \mathrm{wt}_{i,n+1}(\beta) + \frac{i-1}{2} + \beta(n+1) \\ &\equiv \mathrm{wt}_{i,n+1}(\alpha \oplus \beta) + (i-1) + (\alpha(n+1) \oplus \beta(n+1)) \\ &\equiv \mathrm{wt}_{i,n+1}(\alpha \oplus \beta) + i.\end{aligned}$$

The last step holds because $\alpha(n+1) \oplus \beta(n+1) = 1$.

Then,

$$\begin{aligned}&\theta(\alpha, i) + \theta(\alpha, j) + \theta(\beta, i) + \theta(\beta, j) \\ &\equiv \mathrm{wt}_{i,j}(\alpha \oplus \beta) + i + j \\ &\equiv (j - i - 1) + i + j \\ &\equiv 1 \pmod 2.\end{aligned}$$

Therefore,

$$(-1)^{\theta(\alpha,i)}z_\gamma^*(-1)^{\theta(\alpha,j)}z_\delta + (-1)^{\theta(\beta,i)}z_\delta(-1)^{\theta(\beta,j)}z_\gamma^* = 0$$

holds and the submatrix $\mathcal{G}_n(\alpha, \beta; i, j)$ is an Alamouti 2×2, which implies column i and column j are orthogonal. The proof is complete. ■

By taking out some submatrices form $\mathcal{G}_n$, we can get a series of atomic M-type CODs.

Theorem 7. *Given n, for arbitrary integer $-1 \le w \le n+1$, let*

$$\mathcal{G}_n^w = \mathcal{G}_n(\alpha_1, \ldots, \alpha_{\binom{n}{w+1}}, \beta_1, \ldots, \beta_{\binom{n}{n-w+1}}; 1 \sim n),$$

where α_i are all vectors in $\mathbb{F}_2^{n+1}$ with weight $w+1$ and the $(n+1)^{th}$ bit 0, β_i are all vectors in $\mathbb{F}_2^{n+1}$ with weight $n-w+2$ and the $(n+1)^{th}$ bit 1. Then $\mathcal{G}_n^w$ is a COD with parameter $[\binom{n}{w+1} + \binom{n}{w-1}, n, \binom{n}{w}]$.

Proof: Since $\mathcal{G}_n^w$ is a submatrix of the orthogonal design $\mathcal{G}_n$, it's sufficient to prove that if some variable exists on one column of $\mathcal{G}_n^w$ then it exists on every column of $\mathcal{G}_n^w$. We will show that all variables with subscript weight w exist on each column of $\mathcal{G}_n^w$.

For any $\alpha \in \mathbb{F}_2^{n+1}$ such that $\alpha(n+1) = 0, \alpha(i) = 1$ for some $1 \le i \le n$, as $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i) = \mathrm{wt}(\alpha) - 1$, then $\mathrm{wt}(\varphi(\alpha, i)) = w$ if and only if $\mathrm{wt}(s) = w + 1$.

For any $\alpha \in \mathbb{F}_2^{n+1}$ such that $\alpha(n+1) = 1$, and $\alpha(i) = 1$ for some $1 \le i \le n$, as $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i \oplus e) = n + 2 - \mathrm{wt}(\alpha)$, then $\mathrm{wt}(\varphi(\alpha, i)) = w$ if and only if $\mathrm{wt}(\alpha) = n - w + 2$.

Finally, there are $\binom{n}{w+1} + \binom{n}{n-w+1} = \binom{n}{w+1} + \binom{n}{w-1}$ rows taken and $\binom{n}{w}$ different variables in it. The proof is complete. ■

Notice that, in the above constructions, $\mathcal{G}_n^{-1} = (0, 0, \ldots, 0)$ is a trivial COD with rate 0 and delay 1.

For fixed number of antennas n, the code rate

$$\frac{\binom{n}{w}}{\binom{n}{w+1} + \binom{n}{w-1}} = \left(\frac{n-w}{w+1} + \frac{w}{n-w+1}\right)^{-1}$$

is an increasing function of w when $-1 \le w \le \lfloor \frac{n}{2} \rfloor$, as well as the decoding delay $\binom{n}{w}$. Since the decoding delay $\binom{n}{w}$ grows very fast when w is increasing, the sacrifice in rate might be worth the trade-off for a smaller decoding delay in practice.

For example, letting $n = 14$, $w = 0, 1, \ldots, 7$ respectively, we obtain codes with the following parameters with rate decreasing and delay incresing.

TABLE I
CODE RATE AND DELAY FOR $n = 14$

w	k	rate = k/p	delay = p
0	1	0.071	14
1	14	0.152	92
2	91	0.241	378
3	364	0.333	1092
4	1001	0.423	2366
5	2002	0.500	4004
6	3003	0.553	5434
7	3432	0.571	6006

Taking $w = m$ when $n = 2m$ or $2m - 1$, it's easy to verify $\mathcal{G}_n^w$ has parameter $[\binom{2m}{m-1}, 2m-1, \binom{2m-1}{m-1}]$ when $n = 2m - 1$ and $[2\binom{2m}{m-1}, 2m, 2\binom{2m-1}{m-1}]$ when $n = 2m$ with code rate $(m+1)/(2m)$. By Theorem 4 and Theorem 5, we know $\mathcal{G}_n^m$ reaches the maximal rate and it reaches the minimal delay when $n \not\equiv 0 \pmod 4$.

Like the Alamouti 2×2 in [7], certain CODs enjoy a property known as transceiver signal linearization, which can facilitate decoding. This linearization allows the code to be backward compatible with existing signal processing techniques and standards, and allows for the design of low

complexity interference suppressing filters and channel equalizers [18]. It has been shown that a complex orthogonal design can achieve transceiver signal linearization if and only if each row in the code has either all conjugated entries or all non-conjugated entries [18], which is called conjugation separated. Note that $\mathcal{G}_n$ and $\mathcal{G}_n^w$ are all conjugation separated and thus satisfy the transceiver signal linearization property.

When $n \equiv 0 \pmod 4$, it's possible to pad an extra column on $\mathcal{G}_{n-1}$ to obtain a new COD.

Theorem 8. *For positive integer $n = 2m, m$ even, let $\mathcal{H}_n = (\mathcal{G}_{n-1}, \mathcal{L}_n)$, where*

$$\mathcal{L}_n(\alpha) = \alpha(n)(-1)^{\psi(\alpha)} z_{\alpha\oplus e_n}, \text{ for all } \alpha \in \mathbb{F}_2^n$$

and $\psi(\alpha) = \sum_{i=1}^m \alpha(2i)$. Then $\mathcal{H}_n$ is a COD with parameter $[2^n, n, 2^{n-1}]$.

Proof: From Theorem 6, we claim columns in $\mathcal{G}_{n-1}$ are pairwise orthogonal. By proving column $\mathcal{L}_n$ is orthogonal to the other columns, we can complete the proof. It's obvious that each variable exists on $\mathcal{L}_n$ only once. It only remains to prove any two nonzero elements(one is on $\mathcal{L}_n$) in the same row are in an Alamouti 2×2.

Consider column $1 \le i \le n-1$ and column n. For row $\alpha \in \mathbb{F}_2^n$ and $\alpha(i) = \alpha(n) = 1$, $\mathcal{H}_n(\alpha, i) = (-1)^{\theta(\alpha,i)} z^*_{\varphi(\alpha,i)}$ and $\mathcal{H}_n(\alpha, n) = (-1)^{\psi(\alpha)} z_{\alpha\oplus e_n}$. Since each variable exists in $\mathcal{L}_n$, there exists an integer $\beta \in \mathbb{F}_2^n, \beta(n) = 1$ such that $|\mathcal{H}_n(\beta, n)| = |\mathcal{H}_n(\alpha, i)|^*$, which is

$$\beta \oplus e_n = \alpha \oplus \alpha(n)e \oplus e_i.$$

Noting that $\alpha(n) = 1$, thus,

$$\beta = \alpha \oplus e \oplus e_i \oplus e_n. \tag{7}$$

which implies $\beta(i) = \beta(n) = 1$. Now, we calculate the subscript of the variable in $\mathcal{H}_n(\beta, i)$.

$$\begin{aligned} \varphi(\beta, i) &= \beta \oplus \beta(n)e \oplus e_i \\ &= \alpha \oplus e \oplus e_i \oplus e_n \oplus e \oplus e_i \\ &= \alpha \oplus e_n, \end{aligned}$$

which is equal to the subscript of variable in $\mathcal{H}_n(\alpha, n)$. Therefore, the submatrix $\mathcal{H}_n(\alpha, \beta; i, n)$ could be written as follows

$$\begin{pmatrix} (-1)^{\theta(\alpha,i)} z^*_\gamma & (-1)^{\psi(\alpha)} z_\delta \\ (-1)^{\theta(\beta,i)} z^*_\delta & (-1)^{\psi(\beta)} z_\gamma, \end{pmatrix},$$

where $\gamma = \alpha \oplus e_i \oplus e_n$ and $\delta = \alpha \oplus e_n$. Let's check the signs to verify whether it's an Alamouti 2×2.

When i is even,

$$\begin{aligned} &\theta(\alpha, i) + \psi(\alpha) + \theta(\beta, i) + \psi(\beta) \\ \equiv\ &\mathrm{wt}_{i,n}(\alpha) + \frac{i}{2} + \sum_{k=0}^m \alpha(2k) + \mathrm{wt}_{i,n}(\beta) + \frac{i}{2} + \sum_{k=1}^m \beta(2k) \\ \equiv\ &\mathrm{wt}_{i,n}(\alpha \oplus \beta) + \sum_{k=1}^m (\alpha(2k) \oplus \beta(2k)) \\ \equiv\ &(n - i - 1) + (m - 1) && \text{by (7)} \\ \equiv\ &1 \pmod 2. \end{aligned}$$

When i is odd,

$$\begin{aligned} &\theta(\alpha, i) + \psi(\alpha) + \theta(\beta, i) + \psi(\beta) \\ \equiv\ &\mathrm{wt}_{i,n}(\alpha) + \frac{(i-1}{2} + \alpha(n) + \sum_{k=1}^m \alpha(2k) + \\ &\mathrm{wt}_{i,n}(\beta) + \frac{i-1}{2} + \beta(n) + \sum_{k=1}^m \beta(2k) \\ \equiv\ &\mathrm{wt}_{i,n}(\alpha \oplus \beta) + (\alpha \oplus \beta)(n) + \sum_{k=1}^m (\alpha(2k) \oplus \beta(2k)) \\ \equiv\ &(n - i - 1) + 0 + (m - 2) && \text{by (7)} \\ \equiv\ &1 \pmod 2. \end{aligned}$$

Therefore,

$$(-1)^{\theta(\alpha,i)} z_\gamma (-1)^{\psi(\alpha)} z_\delta + (-1)^{\theta(\beta,i)} z_\delta (-1)^{\psi(\beta)} z_\gamma = 0$$

holds and the submatrix $\mathcal{H}_n(\alpha, \beta; i, n)$ an Alamouti 2×2, which implies column i and column n are orthogonal. The proof is complete. ■

Similar with the idea in Theorem 7, by taking out some submatrices of $\mathcal{H}_n$, we can obtain new ones.

Theorem 9. *For positive integer $n = 2m, m$ even, let*

$$\mathcal{H}_n^m = \mathcal{H}_n(\alpha_1, \ldots, \alpha_{\binom{n}{m+1}}; 1, \ldots, n),$$

where α_i are all vectors in $\mathbb{F}_2^n$ with weight $m+1$. Then $\mathcal{H}_n^m$ is a COD with parameter $[\binom{n}{m+1}, n, \binom{n-1}{m}]$.

Proof: From Theorem 8, we know $\mathcal{H}_n$ is orthogonal. Now we will prove that every variable with subscript weight m exists on each column, which implies $\mathcal{H}_n^m$ is a COD.

For $\alpha \in \mathbb{F}_2^n, \alpha(n) = 0, 1 \le i \le n-1$ and $\alpha(i) = 1$, since $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i) = \mathrm{wt}(\alpha) - 1$, then $\mathrm{wt}(\varphi(\alpha, i)) = m$ if and only if $\mathrm{wt}(\alpha) = m + 1$.

For $\alpha \in \mathbb{F}_2^n, \alpha(n) = 1, 1 \le i \le n-1$ and $\alpha(i) = 1$, since $\mathrm{wt}(\varphi(\alpha, i)) = \mathrm{wt}(\alpha \oplus e_i \oplus e) = n + 1 - \mathrm{wt}(\alpha)$, then $\mathrm{wt}(\varphi(\alpha, i)) = m$ if and only if $\mathrm{wt}(\alpha) = n + 1 - m = m + 1$.

For the last column, since $\mathcal{L}_n(\alpha) = (-1)^{\psi(\alpha)} z_{\alpha\oplus e_n}$ for $\alpha(n) = 1$, it's easy to see if $\mathrm{wt}(\alpha) = m+1$, then $\mathrm{wt}(\psi(\alpha)) = 2m$ and vice versa. Therefore, the proof is complete. ■

By Theorem 4 and Theorem 5, we know $\mathcal{H}_n^m$ reaches the maximal rate and minimal delay when $n \equiv 0 \pmod 4$. Up to now, all maximal rate, minimal delay CODs are contained in our constructions, which are $\mathcal{G}_n^m$ when $n \not\equiv 0 \pmod 4$ and $\mathcal{H}_n^m$ when $n \equiv 0 \pmod 4$.

It's worth noticing that, for a given row, there are both conjugated and non-conjugated nonzero entries in $\mathcal{H}_n$ and $\mathcal{H}_n^m$, which violets the transceiver signal linearization property.

In [4], Adams et al. proved that when $n \equiv 1, 2, 3 \pmod 4$, maximal rate CODS with transceiver linearization can achieve the minimal delay, and when $n \equiv 0 \pmod 4$, it can not. Our explicit-form constrictions are consist with their results.

The CODs constructed by Liang in [14], and by Su and Xia in [20] are the same with $\mathcal{G}_n^m$ under equivalence operation,

which achieves maximal rate and minimal delay when $n \not\equiv 0 \pmod 4$. The closed-form constructions in [16] are equivalent to $\mathcal{G}_n^m$ and $\mathcal{H}_n^m$, and therefore achieve maximal rate and minimal delay for any n. The constructions in [3] by Adams et al. have rate $1/2$ and delay 2^{m-1} or 2^m, depending on the parity of n modulo 8. Those rate $1/2$ CODs have smaller decoding delay compared to $\mathcal{G}_n^w$ with rate not less than $1/2$.

IV. An Upper Bound of $A_{\mathbb{C}}(R, n)$

In practice, complex orthogonal design are used to construct high-rate and low decoding complexity space-time block codes with full diversity. It's necessary to take the memory requirements into account, which means that given the number of antennas n and the rate R, we must minimize the decoding delay p. Therefore, we have the following definition.

Definition 10. *[22] For a given R and n, we define $A_{\mathbb{C}}(R, n)$ the minimum number p for which there exists a complex orthogonal design of size $p \times n$ and rate at least R. If no such orthogonal design exists, we define $A_{\mathbb{C}}(R, n) = \infty$.*

The question of the computation of the value $A_{\mathbb{C}}(R, n)$ is addressed as the *fundamental question of complex orthogonal design theory* in [22]. In [14], the author proposes the problem to determine $\hbar_{\mathbb{C}}(p, n)$, where $\hbar_{\mathbb{C}}(p, n)$ denote the maximum number k such that a $[p, n, k]$ complex orthogonal design $\mathcal{O}_z$ exists when n and p is given. And the value of $\hbar_{\mathbb{C}}(p, n)$ is calculated for $n \le 4$. However, the value of $\hbar_{\mathbb{C}}(p, n)$ for $p \ge n \ge 5$ is still unknown.

In fact, if either $A_{\mathbb{C}}(R, n)$ or $\hbar_{\mathbb{C}}(p, n)$ is determined, the other can be easily calculated, as the following proposition reveals.

Proposition 11. *For any positive integer n, and positive real number R, we have*

$$A_{\mathbb{C}}(R, n) = \min_{\hbar_{\mathbb{C}}(p,n) \ge pR} \{p\},$$

or equivalently,

$$\hbar_{\mathbb{C}}(p, n) = \max_{A_{\mathbb{C}}(R,n) \le p} \{R A_{\mathbb{C}}(R, n)\}.$$

Proof: From the definition of $A_{\mathbb{C}}(R, n)$ and $\hbar_{\mathbb{C}}(p, n)$, we can write

$$A_{\mathbb{C}}(R, n) = \min_{\text{COD } [p,n,k] \text{ exists}, \frac{k}{p} \ge R} \{p\}$$

and

$$\hbar_{\mathbb{C}}(p, n) = \max_{\text{COD } [p,n,k] \text{ exits}} \{k\}.$$

Therefore,

$$\begin{aligned} \min_{\hbar_{\mathbb{C}}(p,n) \ge pR} \{p\} &= \min_{\max_{\text{COD } [p,n,k] \text{ exits}} \{k\} \ge pR} \{p\} \\ &= \min_{\text{COD } [p,n,k] \text{ exits}, k \ge pR} \{p\} \\ &= A_{\mathbb{C}}(R, n) \end{aligned}$$

The other equality is similar to prove. ∎

Now, we only consider $A_{\mathbb{C}}(R, n)$. Because $A_{\mathbb{C}}(R, n)$ and $\hbar_{\mathbb{C}}(p, n)$ are related by the previous proposition, an upper bound of $A_{\mathbb{C}}(R, n)$ will induce a lower bound of $\hbar_{\mathbb{C}}(p, n)$ and vice versa.

Since two complex orthogonal designs with parameters $[p_1, n, k_1]$ and $[p_2, n, k_2]$ can be combined to obtain a new complex orthogonal design $[p_1 + p_2, n, k_1 + k_2]$, the inequality

$$A_{\mathbb{C}}(R, n) \le A_{\mathbb{C}}(R_1, n) + A_{\mathbb{C}}(R_2, n)$$

holds, where

$$R = \frac{R_1 A_{\mathbb{C}}(R_1, n) + R_2 A_{\mathbb{C}}(R_2, n)}{A_{\mathbb{C}}(R_1, n) + A_{\mathbb{C}}(R_2, n)}.$$

Combining the above inequality and the fact that $A_{\mathbb{C}}(R, n)$ is an increasing function when n is fixed, a general upper bound of $A_{\mathbb{C}}(R, n)$ can be derived when upper bounds on several points are determined.

The following corollary gives an upper bound on $A_{\mathbb{C}}(R, n)$, which is a consequence of our constructions.

Corollary 12. *For any positive integer $n = 2m$ or $2m - 1$ and any real number $\frac{1}{n} \le R \le \frac{m+1}{2m}$, we have*

$$A_{\mathbb{C}}(R, n) \le \binom{n}{w+1} + \binom{n}{w-1}, \tag{8}$$

where

$$w = \left\lceil \frac{n}{2} - \frac{1}{2}\sqrt{\frac{(n+2)(n+2-2Rn)}{2R+1}} \right\rceil.$$

Especially, if $n \equiv 0 \pmod 4$, we have

$$A_{\mathbb{C}}(R, n) \le \binom{n}{n/2+1}. \tag{9}$$

Proof: Consider COD $\mathcal{G}_n^w[\binom{n}{w+1} + \binom{n}{w-1}, n, \binom{n}{w}]$ with code rate $(\frac{n-w}{w+1} + \frac{w}{n-w+1})^{-1}$. Let $(\frac{n-w}{w+1} + \frac{w}{n-w+1})^{-1} \ge R$, which is equivalent to

$$w^2 - nw + \frac{(Rn-1)(n+1)}{2R+1} \le 0. \tag{10}$$

Solving inequality (10), we have

$$\frac{n(2R+1) - \sqrt{\Delta}}{4R+2} \le w \le \frac{n(2R+1) + \sqrt{\Delta}}{4R+2},$$

where

$$\Delta = (2R+1)(n+2)(n+2-2Rn).$$

Recalling $R \ge 1/n$, it's easy to see $\frac{n(2R+1)-\sqrt{\Delta}}{4R+2} \ge 0$ as $n^2(2R+1)^2 - \Delta = (2R+1)(Rn-1)(n+1) \ge 0$.

From COD $\mathcal{G}_n^w$, we claim there exists a complex orthogonal design $[\binom{n}{w+1} + \binom{n}{w-1}, n, \binom{n}{w}]$, and the corresponding code rate not less than R, which implies $A_{\mathbb{C}}(R, n) \le \binom{n}{w+1} + \binom{n}{w-1}$.

Upper bound (9) is similar to prove by COD $\mathcal{H}_n^m$. ∎

V. Conclusion

In this paper, we present a systematic explicit-form construction of complex orthogonal space-time block codes for any number of antennas. In space-time block code, code rate and decoding delay are two basic and important parameters. Our constructions contain those with maximal code rate and minimal decoding delay. Besides that, the constructions contain codes sacrificing some code rate to achieve shorter decoding delay, which first systematically demonstrates the tradeoff between code rate and decoding delay.

Based on our constructions, an upper bound of $A_{\mathbb{C}}(R,n)$ is derived. Up to now, for general R and n, the exact value of $A_{\mathbb{C}}(R,n)$ is still unknown, which will be our future research.

VI. Acknowledgement

This work was supported by the National Natural Science Foundations of China (Grant Nos. 61170208 and 60832001), Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20090071110073), Fox Ying Yung Education Foundation (Grant No. 114401), and Shu Guang Project supported by Shanghai Municipal Education Commission and Shanghai Education Development Foundation (Grant No. 10SG01).

References

[1] J. F. Adams, "Vector fields on spheres," Ann. Math., vol. 75, no. 2, pp. 603-632, 1962.

[2] J. F. Adams, P. D. Lax, and R. S. Phillips, "On matrices whose real linear combinations are nonsingular," in Proc. Amer. Math. Soc., vol. 16, 1965, pp. 318-322.

[3] S. S. Adams, J. Davis, N. Karst, M. K. Murugan, B. Lee, M. Crawford, C. Greeley, "Novel classes of minimal delay and low PAPR rate 1/2 complex orthogonal designs," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2254-2262, Apr. 2011.

[4] S. S. Adams, N. Karst, M. K. Murugan and T. A. Wysocki, "On transceiver signal linearization and the decoding delay of maximum rate complex orthogonal space-time block codes," IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3618-3621, Jun. 2011.

[5] S. S. Adams, N. Karst, and J. Pollack, "The minimum decoding delay of maximum rate complex orthogonal space-time block codes," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2677-2684, Aug. 2007.

[6] S. S. Adams, N. Karst, M. K. Murugan., "The final case of the decoding delay problem for maximum rate complex orthogonal designs," IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 103-122, Jan. 2010.

[7] S. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Select. Areas Commun., vol. 16, pp. 1451-1458, Oct. 1998.

[8] A. V. Geramite and N. J. Pullman, "Orthogonal Designs: Quadratic Forms and Hadamard Matrices (Lecture Notes in Pure and Applied Mathematics)," New York: Marcel Dekker, vol. 43, 1979.

[9] R. L. Graham, D. E. Knuth and O. Patashnik, "Concrete Mathematics: A Foundation for Computer Science," 2nd Edition, Pearson Education, 1994.

[10] R. A. Horn and C. R. Johnson, "Topics in Matrix Analysis," Cambridge, U.K.: Cambridge Univ. Press, 1991.

[11] M. Z. A. Khan, B. S. Rajan, "A generalization of some existence results on orthogonal designs for STBCs," IEEE Trans. Inf. Theory, vol. 50, no. 1, Jan. 2004.

[12] H. Kan and H. Shen, "A counterexample for the open problem on the minimal delays of orthogonal designs with maximal rates," IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 355-359, Jan. 2005.

[13] H. Kan and H. Shen, "Lower bounds on the minimal delay of complex orthogonal designs with maximal rats," IEEE Trans. Commun., vol. 54, no. 3, pp. 383-388, Mar. 2006.

[14] X-B. Liang, "Orthogonal designs with maximal rates," IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2468-2503, Oct. 2003.

[15] Y. Li, H. Kan, C. Yuan and H. Ma, "The maximal rates and minimal decoding delay of more general complex orthogonal designs," Science in China, Series F: Information Sciences 2010, pp. 1826-1832.

[16] K. Lu, S. Fu, and X. G. Xia, "Closed-form designs of complex orthogonal space-time block codes of rates (k+1)/(2k) for 2k-1 or 2k transmit antennas," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4340-4347, Dec. 2005.

[17] S. K. Mohammed, B. S. Rajan and A. Chockalingam, "On the maximal rate of non-square STBCs from complex orthogonal designs," in Proc. IEEE Global Telecommun. Conf. (GLOBECOM '07), Nov. 2007, pp. 1709-1713.

[18] W. Su, S. N. Batalama, and D. A. Pados, "On orthogonal space-time block codes and transceiver signal linearization," IEEE Commun. Lett. vol. 8, no. 60, pp. 458-460, Feb. 2004.

[19] W. Su and X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rates 7/11 and 3/5 for 5 and 6 transmit antennas", IEEE Trans. Inf. Theory, vol. 69, no. 1, pp. 313 - 316, Jan. 2002.

[20] W. Su, X.-G. Xia, and K. J. R. Lui, "A systematic design of high-rate complex orthogonal space-time block codes," IEEE Commun. Lett. vol. 8, no. 6, pp. 380-382, Jun. 2004.

[21] J. Seberry, S. A. Spence, and T. A. Wysocki, "A construction technique for generalized complex orthogonal designs and applications to wireless communications," Linear Algebra and its Applications 405 (2005) 163-167.

[22] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1456-1467, July 1999.

[23] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Correction to 'Space-time block codes from orthogonal designs,'" IEEE Trans. Inf. Theory, vol. 46, no. 1, Jan. 2000.

[24] L. C. Tran, T. A. Wysocki, J. Seberry, A. Mertins and S. S. Adams, "Novel constructions of improved square complex orthogonal designs for eight transmit antennas," IEEE Trans. Inf. Theory, vol. 55, no. 10, Oct. 2009.

[25] W. Su, X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rate 7/11 and 3/5 for 5 and 6 transmit antennas," IEEE Trans. Inf. Theory, vol. 49, pp. 313-316, Jan. 2003.